Claims

1. A system for identifying principals within a computing environment, the system comprising:

a plurality of principal objects, wherein each principal object corresponds to a specific principal authenticated to perform a digital action within the computing environment and wherein each principal object is operable for use by a computer process within the computing environment to associate a plurality of resource objects with the specific principal corresponding to the principal object; and

a plurality of identity claims, wherein each identity claim uniquely identifies the specific principal corresponding to each specific principal object, and wherein at least one of the plurality of principal objects comprises two or more identity claims each uniquely identifying the specific principal corresponding to the at least one principal object.

2. A system as defined in claim 1, further comprising:

a plurality of identity references, wherein each of the plurality of identity references is associated with a resource object within the computing environment, and wherein each of the plurality of identity references identify the associated resource object as being associated with a specific principal based on a link assertion within the identity reference to a specific identity claim.

3. A system as defined in claim 2, wherein each of the plurality of identity claims comprises a type assertion and a value assertion that collectively identify the specific principal corresponding to the principal object to which each of the identity claims are associated.

4. A system as defined in claim 3, wherein the link assertion within each of the plurality of the identity references comprises the type assertion and the value assertion specified in the specific identity claim to which each identity reference is linked.

5. A system as defined in claim 4, wherein a first type assertion for a first identity claim associated with a first principal object indicates that the value assertion in the first identity

claim comprises an electronic mail address uniquely associated with a first principal corresponding to the first principal object.

6. A system as defined in claim 5, wherein the first identity claim further comprises a start time reference assertion indicating a point in time when the email address was initially associated with the first principal.

7. A system as defined in claim 6, wherein the first identity claim further comprises an end time reference assertion indicating a point in time when the association between the email address and the first principal lapses.

8. A system as defined in claim 4, wherein a second type assertion for a second identity claim associated with the first principal object indicates that the value assertion in the second identity claim comprises a telephone number uniquely associated with the first principal.

9. A system as defined in claim 2, wherein the computing environment is a distributed computing system, and wherein at least one identity reference is maintained on a computer system different than a computer system on which the identity claim linked to the identity reference is maintained.

10. A system for identifying a first principal within a computing environment, wherein the first principal is authenticated to perform a digital action within the computing environment, the system comprising:

a first principal object corresponding to the first principal, wherein the first principal object is operable for use by a computer process within the computing environment to associate at least one resource object with the first principal;

a plurality of identity claims, wherein each identity claim uniquely identifies the first principal, the first principal object including the plurality of identity claims such that the computer process may associate the at least one resource object with the first principal using any of the plurality of identity claims.

11. A system as defined in claim 10, further comprising:

a first identity reference associated with a first resource object within the computing environment, wherein the first identity reference identifies the first resource object as being associated with the first principal based on a first link assertion within the first identity reference to a first identity claim in the plurality of identity claims.

12. A system as defined in claim 11, further comprising:

a second identity reference associated with a second resource object within the computing environment, wherein the second identity reference identifies the second resource object as being associated with the first principal based on a second link assertion within the second identity reference to the first identity claim.

13. A system as defined in claim 12, wherein the first resource object represents a file associated with a first application program and the second resource object represents a file associated with a second application program.

14. A system as defined in claim 13, wherein the first application program is a word processing application program.

15. A system as defined in claim 12, wherein each of the plurality of identity claims comprises a type assertion and a value assertion that collectively specify the first principal, and wherein the first and second link assertions comprise the type assertion and the value assertion specified in the identity claim to which the first and the second identity references are linked.

16. A system as defined in claim 15, wherein a first type assertion for the first identity claim indicates that the value assertion in the first identity claim comprises an electronic mail address uniquely associated with the first principal.

17. A system as defined in claim 16, wherein the first identity claim further comprises:

a start time reference assertion indicating a point in time when the email address was initially associated with the first principal; and

an end time reference assertion indicating a point in time when the association between the email address and the first principal lapses.

18. A system as defined in claim 10, wherein the first principal is selected from the group consisting of an individual, an organization and a module within the computing environment.

19. A system as defined in claim 10, wherein the computing environment is a distributed computing system.

20. A system as defined in claim 10, wherein the computing environment is a stand-alone computing system.

21. A computer readable medium having a data structure stored thereon for use in identifying a principal authenticated to perform a digital action within a computing environment, the data structure comprising:

a value assertion uniquely identifying the principal within a particular identification scheme;

a type assertion indicating the particular identification scheme corresponding to the value assertion; and

a time reference assertion specifying a time frame in which the principal is uniquely identified by the value assertion within the particular identification scheme.

22. A computer readable medium as defined in claim 21, wherein the data structure represents an identity claim that associates a principal object with the principal, wherein the principal object is operable for use by a computer process within the computing environment to associate at least one resource object with the principal.

23. A computer readable medium as defined in claim 22, wherein the time reference comprises:

a start time reference assertion indicating a point in time when the value assertion was initially associated with the principal; and

an end time reference assertion indicating a point in time when the association between the value assertion and the principal lapses.

24. A computer readable medium as defined in claim 22, the data structure further comprising:

a display assertion specifying the value assertion in a form recognizable to human users within the computing environment, wherein the computer process displays the display assertion to a user in response to a request by the user to view the association between the principal and the at least one resource object.

25. A computer readable medium as defined in claim 21, wherein the principal is selected from the group consisting of an individual, an organization and a module within the computing environment.

26. A computer readable medium as defined in claim 21, wherein the type assertion indicates that the value assertion comprises an electronic mail address uniquely associated with the principal.

27. A computer readable medium as defined in claim 21, wherein the type assertion indicates that the value assertion comprises a telephone number uniquely associated with the principal.

28. A method for identifying a first principal authenticated to perform a digital action within a computing environment, the method comprising:

creating a principal object operable for use by a computer process within the computing environment to identify the first principal as being associated with a plurality of resource objects maintained within the computing environment;

associating with the principal object a first identity claim uniquely identifying the first principal within a particular identification scheme, wherein unique identification of the first principal within the particular identification scheme is accomplished by assignment of unique identification strings to each of a plurality of principals;

receiving a plurality of resource objects associated with a plurality of application programs, wherein each of the plurality of resource objects are associated with an identity reference comprising a declaration that links each resource object to the principal object; and

identifying within the computing environment each of the plurality of resource objects as being associated with the first principal based on the declaration links contained in the associated identity references, wherein the computer process utilizes identification of each of the plurality of resource objects to the first principal to perform at least one task in connection with each identified resource object.

29. A method as defined in claim 28, wherein the receiving act comprises:

receiving a first resource object having associated therewith a first identity reference linked to the first identity claim based on a first declaration comprising a unique identification string assigned to the first principal, wherein the first resource object represents a first file associated with a first application program; and

receiving a second resource object having associated therewith a second identity reference linked to the first identity claim based on a second declaration comprising the unique identification string assigned to the first principal, wherein the second resource object represents a second file associated with a second application program.

30. A method as defined in claim 29, wherein the identifying act comprises:

identifying the first file and the second file as being associated with the first principal based on the linking of the first identity reference and the second identify reference to the first identity claim.

31. A method as defined in claim 28, further comprising:

associating with the principal object properties associated with the first principal, wherein the task performed by the computer process in response to the identifying act comprises an act of displaying a graphical representation of the properties associated with the first principal in conjunction with a graphical representation of at least one of the plurality of resources linked to the principal object.

32. A method as defined in claim 30, further comprising:

associating with the principal object properties associated with the first principal, wherein the task performed by the computer process in response to the identifying act comprises an act of authenticating access by the first principal to at least one of the plurality of resources linked to the principal object.

33. A method as defined in claim 28, wherein the creating act comprises:

creating a phantom principal object in response to receiving a resource object having a identity reference comprising a declaration that does not link the resource object to the principal object, the declaration comprising an identification string uniquely identifying a second principal within the particular identification scheme, and wherein the phantom principal object is created to include the identification string assigned to the second principal; and

saving the phantom principal object to a data store containing the principal object corresponding to the first principal.

34. A method as defined in claim 33, further comprising:

receiving a second principal object, wherein the second principal object comprises a second identity claim that comprises the identification string assigned to the second principal; and

in response to determining that the phantom principal object and the second principal both correspond to the second principal, deleting the phantom principal object from the data store and saving to the data store the second principal object such that the second principal object is operable for use by the identifying act.

35. A method as defined in claim 28, wherein the first identity claim is stored in the computing environment in a data store, the method further comprising:

in response to receiving a second identity claim for storage into the data store, determining whether the second identity claim and the first identity claim both specify an identical unique identification string; and

in response to determining that both the first identity claim and the second identity claim specify the identical unique identification string, invoking a fault resolution process to determine a primary identity claim that is to be stored in the data store and available to the identifying act.

36. A method as defined in claim 35, wherein the invoking act comprises:

merging data stored in the second identity claim into the first identity claim.

37. A method as defined in claim 35, wherein the invoking act comprises:

deleting the first identity claim; and

storing in the data store the second identity claim.

38. A computer program product readable by a computer system and tangibly embodying a program of instructions executable by the computer system to perform the method of claim 28.